

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 24 January 2001 (24.01.01)	
International application No. PCT/DE00/01788	Applicant's or agent's file reference 99P2055P
International filing date (day/month/year) 31 May 2000 (31.05.00)	Priority date (day/month/year) 15 June 1999 (15.06.99)
Applicant HORN, Günther et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
 25 October 2000 (25.10.00)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

BEST AVAILABLE COPY

The International Bureau of WIPO
 34, chemin des Colombettes
 1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Form PCT/IB/331 (July 1992)

Authorized officer

Maria Kirchner

Telephone No.: (41-22) 338.83.38

DE0001788

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 99P2055P	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/DE 00/ 01788	Internationales Anmeldedatum (Tag/Monat/Jahr) 31/05/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 15/06/1999
Anmelder SIEMENS AKTIENGESELLSCHAFT		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbaren **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 3



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

PCT-ANTRAG

99P2055P

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

0	Vom Anmeldeamt auszufüllen	
0-1	Internationales Aktenzeichen.	PTO/PCT Rec'd 17 DEC 2001
0-2	Internationales Anmeldedatum	
0-3	Name des Anmeldeamts und "PCT International Application"	
0-4	Formular - PCT/RO/101 PCT-Antrag	
0-4-1	erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 08.03.2000)
0-5	Antragsersuchen Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird	
0-6	(Vom Anmelder gewähltes) Anmeldeamt	Deutsches Patent- und Markenamt (RO/DE)
0-7	Aktenzeichen des Anmelders oder Anwalts	99P2055P
I	Bezeichnung der Erfindung	VERFAHREN UND ANORDNUNG ZUR ÜBERPRÜFUNG EINER AUTHENTIZITÄT EINES ERSTEN KOMMUNIKATIONSTEILNEHMERS IN EINEM KOMMUNIKATIONSNETZ
II	Anmelder	
II-1	Diese Person ist	nur Anmelder
II-2	Anmelder für	Alle Bestimmungsstaaten mit Ausnahme von US
II-4	Name	SIEMENS AKTIENGESELLSCHAFT
II-5	Anschrift:	Wittelsbacherplatz 2 D-80333 München Deutschland
II-6	Staatsangehörigkeit (Staat)	DE
II-7	Sitz/Wohnsitz (Staat)	DE
II-8	Telefonnr.	(089) 636-82819
II-9	Telefaxnr.	(089) 636-81857

PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

III-1	Anmelder und/oder Erfinder	
III-1-1	Diese Person ist	Anmelder und Erfinder
III-1-2	Anmelder für	Nur US
III-1-4	Name (FAMILIENNAME, Vorname)	HORN, Günther
III-1-5	Anschrift:	Eduard-Schmid-Str. 16 D-81541 München Deutschland
III-1-6	Staatsangehörigkeit (Staat)	DE
III-1-7	Sitz/Wohnsitz (Staat)	DE
III-2	Anmelder und/oder Erfinder	
III-2-1	Diese Person ist	Anmelder und Erfinder
III-2-2	Anmelder für	Nur US
III-2-4	Name (FAMILIENNAME, Vorname)	CUELLAR, Jorge
III-2-5	Anschrift:	Höllriegelskreuther Weg D-82065 Baierbrunn Deutschland
III-2-6	Staatsangehörigkeit (Staat)	DE
III-2-7	Sitz/Wohnsitz (Staat)	DE
IV-1	Anwalt oder gemeinsamer Vertreter; oder besondere Zustellanschrift Die unten bezeichnete Person ist/wird hiermit bestellt, um den (die) Anmelder vor den internationalen Behörden zu vertreten, und zwar als:	gemeinsamer Vertreter
IV-1-1	Name	SIEMENS AKTIENGESELLSCHAFT
IV-1-2	Anschrift:	Wittelsbacherplatz 2 D-80333 München Deutschland
IV-1-3	Telefonnr.	(089) 636-82819
IV-1-4	Telefaxnr.	(089) 636-81857
V	Bestimmung von Staaten	
V-1	Regionales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE und jeder weitere Staat, der Mitgliedsstaat des Europäischen Patentübereinkommens und Vertragsstaat des PCT ist
V-2	Nationales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	AU BR CN IN JP KR US

PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

V-5	Erklärung bzgl. vorsorglicher Bestimmungen Zusätzlich zu den unter Punkten V-1, V-2 und V-3 vorgenommenen Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der nachstehend unter Punkt V-6 angegebenen Staaten. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt.		
V-6	Staaten, die von der Erklärung über vorsorgliche Bestimmungen ausgenommen werden	KEINE	
VI-1	Priorität einer früheren nationalen Anmeldung beansprucht		
VI-1-1	Anmeldedatum	15 Juni 1999 (15.06.1999)	
VI-1-2	Aktenzeichen	19927271.9	
VI-1-3	Staat	DE	
VI-2	Ersuchen um Erstellung eines Prioritätsbeleges Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der in der (den) nachstehend genannten Zeile(n) bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln:	VI-1	
VII-1	Gewählte Internationale Recherchenbehörde	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	Kontrollliste	Anzahl der Blätter	Elektronische Datei(en) beigelegt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	13	-
VIII-3	Ansprüche	2	-
VIII-4	Zusammenfassung	1	99_p_2055_p.txt
VIII-5	Zeichnung(en)	4	-
VIII-7	INSGESAMT	24	
VIII-8	Beigelegte Unterlagen	Unterlage(n) in Papierform beigelegt	Elektronische Datei(en) beigelegt
VIII-16	Blatt für die Gebührenberechnung	✓	-
VIII-17	PCT-EASY-Diskette	-	Diskette
VIII-17	Sonstige (einzeln aufgeführt):	Kopie der Ursprungsfassung	-
VIII-18	Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll	-	
VIII-19	Sprache der int. Anmeldung	Deutsch	

PCT-ANTRAG

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

IX-1	Unterschrift des Anmelders oder Anwalts	<i>i.V. Marg</i>
IX-1-1	Name	SIEMENS AKTIENGESELLSCHAFT
IX-1-2	Name der unterzeichnenden Person	Margraf
IX-1-3	Eigenschaft	Nr. 144/74 Ang.-AV
IX-2	Unterschrift des Anmelders oder Anwalts	
IX-2-1	Name (FAMILIENNAME, Vorname)	HORN, Günther
IX-3	Unterschrift des Anmelders oder Anwalts	
IX-3-1	Name (FAMILIENNAME, Vorname)	CUELLAR, Jorge

VOM ANMELDEAMT AUSZUFÜLLEN

10-1	Datum des tatsächlichen Eingangs dieser internationalen Anmeldung	
10-2	Zeichnung(en):	
10-2-1	Eingegangen	
10-2-2	Nicht eingegangen	
10-3	Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingeg. Unterlage(n) oder Zeichnung(en) zur Vervollständigung dieser int. Anmeldung	
10-4	Datum des fristgerechten Eingangs der Berichtigung nach PCT Artikel 11(2)	
10-5	Internationale Recherchenbehörde	ISA/EP
10-6	Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben	

VOM INTERNATIONALEN BÜRO AUSZUFÜLLEN

11-1	Datum des Eingangs des Aktenexemplars beim Internationalen Büro	
------	---	--

**PCT (ANHANG - BLATT FÜR DIE
GEBÜHRENBERECHNUNG)**

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

(Dieses Blatt zählt nicht als Blatt der internationalen Anmeldung und ist nicht Teil derselben)

0	Vom Anmeldeamt auszufüllen		
0-1	Internationales Aktenzeichen.		
0-2	Eingangsstempel des Anmeldeamts		
0-4	Formular - PCT/RO/101 (Anlage)		
0-4-1	PCT Blatt für die Gebührenberechnung erstellt durch Benutzung von	PCT-EASY Version 2.90 (aktualisiert 08.03.2000)	
0-9	Aktenzeichen des Anmelders oder Anwalts	99P2055P	
2	Anmelder	SIEMENS AKTIENGESELLSCHAFT, et al.	
12	Berechnung der vorgeschriebenen Gebühren	Höhe der Gebühr/Multiplikator	Gesamtbeträge (DEM)
12-1	Übermittlungsgebühr T	⇒	175
12-2	Recherchegebühr S	⇒	1.848.26
12-3	Internationale Gebühr Grundgebühr (erste 30 Blätter) b1	799.93	
12-4	Anzahl der Blätter über 30	0	
12-5	Zusatzblattgebühr (X)	17.6	
12-6	Gesamtbetrag der weiteren Gebühren b2	0	
12-7	b1 + b2 = B	799.93	
12-8	Bestimmungsgebühren Anzahl der in der internationalen Anmeldung vorgenommenen Bestimmungen	8	
12-9	Number of designation fees payable (maximum 8)	8	
12-10	Bestimmungsgebühr (X)	172.11	
12-11	Gesamtbetrag der Bestimmungsgebühren D	1.376.88	
12-12	PCT-EASY-Gebührenermäßigung R	-246.43	
12-13	Gesamtbetrag der internationalen Gebühr (B+D-R) I	⇒	1.930.38
12-14	Gebühr für Prioritätsbeleg Anzahl der beantragten Prioritätsbelege	1	
12-15	Gebühr per Prioritätsbeleg (X)	35	
12-16	Gesamtbetrag Gebühr für Prioritätsbeleg(e) P	⇒	35
12-17	Gesamtbetrag der zu zahlenden Gebühren (T+S+I+P)	⇒	3.988.64
12-19	Zahlungsart	Sonstige: Abbuchung durch gesonderte Zahlungsliste	

**PCT (ANHANG - BLATT FÜR DIE
GEBÜHRENBERECHNUNG)**

Original (für EINREICHUNG) - gedruckt am 24.05.2000 03:58:18 PM

12-20	Anweisungen betreffend laufendes Konto Das Anmeldeamt:	Deutsches Patent- und Markenamt (RO/DE)
12-20-2	wird beauftragt, Fehlbeträge oder Überzahlungen des vorstehend angegebenen Gesamtbetrags der Gebühren meinem laufenden Konto zu belasten bzw. gutzuschreiben	✓
12-21	Nummer des laufenden Kontos	409022601
12-22	Datum	24 Mai 2000 (24.05.2000)
12-23	Name und Unterschrift	SIEMENS AKTIENGESSELLSCHAFT <i>i.V. Mory</i>

PRÜFPROTOKOLL UND BEMERKUNGEN

13-2-1	Prüfergebnisse Antrag	Grün? Die Bezeichnung der Erfindung muß kurz und genau gefaßt sein. Bitte überprüfen.
13-2-2	Prüfergebnisse Staaten	Grün? Es können mehr Bestimmungen vorgenommen werden. Die folgenden Staaten sind nicht bestimmt worden: AP: (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW); EA: (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM); OA: (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG); AE, AG, AL, AM, AT, AZ, BA, BB, BG, BY, CA, CH, LI, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW. Bitte überprüfen.

RECEIVED BY
ART 34 AMDT

Patent claims

1. A method for checking the authenticity of a first
5 communication subscriber in a communications network,
 - in which a first fault information item is formed in the
first communication subscriber using a fault detection
data item of the service provider and an information item
relating to a random data item;
 - 10 - in which a second fault information item is formed in a
second communication subscriber in the communications
network using a fault detection data item of the second
communication subscriber and the information item
relating to the random data item;
 - 15 - in which the authenticity of the first communication
subscriber is checked using the first fault information
item and the second fault information item.
2. The method as claimed in claim 1, in which a difference is
20 determined between the fault detection data item of the
first communication subscriber and the fault detection data
item of the second communication subscriber.
3. The method as claimed in claim 2, in which the difference is
25 limited.
4. The method as claimed in one of claims 1 to 3, used within
the scope of a mobile phone system.
- 30 5. An arrangement for checking the authenticity of a first
communication subscriber in a communications network,

- 5 - in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item;

- in which a second communication subscriber is set up in the communications network in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item;
- in which the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

10

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

15

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

20

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

25

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

30

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EP0-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 799 084 A (GALLAGHER MICHAEL D ET AL) 25. August 1998 (1998-08-25) Spalte 5, Zeile 45 -Spalte 6, Zeile 26 -----	1-11
X	WO 91 01067 A (MOTOROLA INC) 24. Januar 1991 (1991-01-24) Seite 4, Zeile 22 -Seite 5, Zeile 22 -----	1,2,4-11

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

4. Oktober 2000

Absendedatum des internationalen Recherchenberichts

17/10/2000

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Bernedo Azpiri, P

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 00/01788

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5799084 A	25-08-1998	NONE	
WO 9101067 A	24-01-1991	AU 6034790 A	06-02-1991
		CA 2063447 A,C	13-01-1991
		IL 94467 A	31-12-1995
		JP 2684118 B	03-12-1997
		JP 5503816 T	17-06-1993
		MX 166091 B	17-12-1992
		US 5239294 A	24-08-1993

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES
INTERNATIONALEN RECHERCHENBERICHTS
ODER DER ERKLÄRUNG

An
SIEMENS AKTIENGESELLSCHAFT
Wittelsbacherplatz 2
80333 München
GERMANY

ZT GG VM Mch P/Ri

Eing. 17. Okt. 2000

GR
Frist

(Regel 44.1 PCT)

*Kognat, zum anerkennen. St. gegeben.
Zur Antrag auf int. Vorläufige Prüf., siehe Sp. 7*

Absendedatum
(Tag/Monat/Jahr)

17/10/2000

Aktenzeichen des Anmelders oder Anwalts

99P2055P

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/DE 00/01788

Internationales Anmeldedatum

(Tag/Monat/Jahr)

31/05/2000

Anmelder

SIEMENS AKTIENGESELLSCHAFT

1. ☒ Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

Einreichung von Änderungen und einer Erklärung nach Artikel 19:

Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20,
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.
3. ☐ Hinsichtlich des Widerspruchs gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß
- ☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsbüro dem Internationalen Büro übermittelt worden sind.
- ☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von 18 Monaten seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90 bis bzw. 90^{bis}3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von 19 Monaten seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von 20 Monaten seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsbüro vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Peggy Frenzel

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen. Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen die anderen Ansprüche nicht neu nummeriert zu werden. Im Fall einer Neunummerierung sind die Ansprüche fortlaufend zu nummerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
"Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigelegt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts 99P2055P	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> WEITERES VORGEHEN </div> <div style="width: 50%;"> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5 </div> </div>	
Internationales Aktenzeichen PCT/DE 00/ 01788	Internationales Anmeldedatum (Tag/Monat/Jahr) 31/05/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 15/06/1999
Anmelder SIEMENS AKTIENGESELLSCHAFT		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 3

☐ wie vom Anmelder vorgeschlagen

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 799 084 A (GALLAGHER MICHAEL D ET AL) 25. August 1998 (1998-08-25) Spalte 5, Zeile 45 -Spalte 6, Zeile 26	1-11
X	WO 91 01067 A (MOTOROLA INC) 24. Januar 1991 (1991-01-24) Seite 4, Zeile 22 -Seite 5, Zeile 22	1,2,4-11

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

4. Oktober 2000

Absendedatum des internationalen Recherchenberichts

17/10/2000

Name und Postanschrift der Internationalen Recherchenbehörde
 Europäisches Patentamt, P.B. 5818 Patentaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Bernedo Azpiri, P

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5799084	A	25-08-1998	KEINE		
WO 9101067	A	24-01-1991	AU	6034790 A	06-02-1991
			CA	2063447 A,C	13-01-1991
			IL	94467 A	31-12-1995
			JP	2684118 B	03-12-1997
			JP	5503816 T	17-06-1993
			MX	166091 B	17-12-1992
			US	5239294 A	24-08-1993

4/PATS

1

Beschreibung**Verfahren und Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz**

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz.

10

In einem Kommunikationsnetz werden im allgemeinen Daten zwischen Kommunikationsteilnehmern, beispielsweise einem Dienstanbieter und einem Dienstanutzer, übertragen. Um ein Kommunikationsnetz vor einem Eindringen eines nichtberechtigten Kommunikationsteilnehmers in das Kommunikationsnetz zu schützen, wird in der Regel die Authentizität eines jeden Kommunikationsteilnehmers überprüft.

Aus Dokument [1] ist ein Verfahren und eine Anordnung zur Überprüfung einer Authentizität eines Kommunikationsteilnehmers, insbesondere eines Dienstansbieters oder eines Dienstanutzers, in einem Kommunikationsnetz bekannt.

Das aus dem Dokument [1] bekannte Verfahren und die entsprechende Anordnung basieren auf einem sogenannten 3G TS 33.102 Version 3.0.0-Draft-Standard, welcher eine Sicherheits-Architektur eines Mobilfunksystems beschreibt.

In Fig.4 ist die Vorgehensweise bei einer Überprüfung einer Authentizität eines Kommunikationsteilnehmers, wie sie aus dem Dokument [1] bekannt ist, symbolhaft dargestellt und wird im folgenden kurz und auszugsweise erläutert.

Eine Übertragung von Daten ist in Fig.4 jeweils durch einen Pfeil dargestellt. Eine Richtung eines Pfeils kennzeichnet eine Übertragungsrichtung bei einer Datenübertragung.

Fig.4 zeigt ein Mobilfunksystem 400, umfassend einen Nutzer 401 einer Kommunikationsdienstleistung, beispielsweise ein Mobiltelefon, und einen Anbieter 402 einer Kommunikationsdienstleistung. Der Anbieter 402 umfaßt ein Einwählnetz 403 mit einem Einwählnetzbetreiber, bei dem der Nutzer 401 lokal eine Kommunikationsdienstleistung anfordert, und ein Heimatnetz 404 mit einem Heimatnetzbetreiber, bei dem der Nutzer 401 angemeldet und registriert ist.

10 Ferner weisen der Nutzer 401, das Einwählnetz 403 und das Heimatnetz 404 jeweils eine zentrale Verarbeitungseinheit mit einem Speicher auf, beispielsweise einen Server (Zentralrechner), mit welcher Verarbeitungseinheit die im folgenden beschriebene Vorgehensweise überwacht und gesteuert wird und
15 auf welchem Speicher Daten gespeichert werden und/oder sind.

Das Einwählnetz 403 und das Heimatnetz 404 sind über eine Datenleitung, über welche digitale Daten übertragen werden können, miteinander verbunden. Der Nutzer 401 und das Einwähl-
20 netz 403 sind über ein beliebiges Übertragungsmedium zur Übertragung von digitalen Daten miteinander verbunden.

Bei einer Kommunikation wählt sich der Nutzer 401 in das Einwählnetz 403 ein 410. Zu Beginn der Kommunikation erfolgt eine
25 Überprüfung sowohl der Authentizität des Nutzers 401 als auch der Authentizität des Anbieters 402.

Dazu fordert das Einwählnetz 403 sogenannte Authentifikationsdaten, mit welchen die Überprüfung der Authentizität des
30 Nutzers 401 und des Anbieters 402 möglich ist, von dem Heimatnetz 404 an 411.

Die Authentifikationsdaten, welche von dem Heimatnetz 404 ermittelt werden, umfassen eine Zufallszahl und eine Sequenz-
35 folgennummer des Anbieters 402. Die Sequenzfolgennummer des Anbieters 402 wird derart ermittelt, daß ein Zähler des Anbieters 402 bei jedem Kommunikationsversuch zwischen dem Nut-

zer 401 und dem Anbieter 402 die Sequenzfolgennummer des Anbieters 402 um den Wert 1 erhöht.

5 Es ist anzumerken, daß die Zufallszahl und die Sequenzfolgennummer des Anbieters 402 nur einen Teil der Authentifikationsdaten darstellen und nicht abschließend zu verstehen sind. Weitere Authentifikationsdaten sind aus [1] bekannt.

10 Das Heimatnetz 404 überträgt die angeforderten Authentifikationsdaten an das Einwählnetz 403 412. Das Einwählnetz 403 bearbeitet die empfangenen Authentifikationsdaten in geeigneter Weise 413 und überträgt die bearbeiteten Authentifikationsdaten an den Nutzer 401 414.

15 Der Nutzer 401 überprüft unter Verwendung einer eigenen Sequenzfolgennummer, welche entsprechend der Sequenzfolgennummer des Anbieters 402 gehandhabt wird, und der Sequenzfolgennummer des Anbieters 402 die Authentizität des Anbieters 402 415.

20 Die Vorgehensweise bei der Überprüfung der Authentizität des Anbieters 402 ist in [1] beschrieben.

Ein Ergebnis der Überprüfung der Authentizität des Anbieters 402, "Authentizität des Anbieters in Ordnung" 416,
25 "Authentizität des Anbieters in Ordnung, aber ein Sequenzfehler aufgetreten" 417 oder "Authentizität des Anbieters nicht in Ordnung" 418, wird von dem Nutzer 401 an den Anbieter 402 übertragen 419.

30 Bei dem Ergebnis "Authentizität des Anbieters in Ordnung" 416 überprüft das Einwählnetz 403, wie es in [1] beschrieben ist, die Authentizität des Nutzers 401 420.

Bei dem Ergebnis "Authentizität des Anbieters nicht in Ordnung" 418 wird die Kommunikation unterbrochen bzw. neu begonnen 421.
35

Bei dem Ergebnis "Authentizität des Anbieters in Ordnung, aber ein Sequenzfehler aufgetreten" 417 erfolgt eine Resynchronisation derart, daß das Heimatnetz 404 eine Resynchronisationsanfrage an den Nutzer 401 sendet 422. Der Nutzer antwortet mit einer Resynchronisationsantwort, bei welcher Resynchronisationsdaten an das Heimatnetz 404 übertragen werden 423. In Abhängigkeit der Resynchronisationsantwort wird die Sequenzfolgenummer des Anbieters 402 verändert 424. Anschließend erfolgt die Prüfung der Authentizität des Nutzers 401, wie es aus [1] bekannt ist.

Die beschriebene Vorgehensweise weist den Nachteil auf, daß bei einer Überprüfung einer Authentizität eines Kommunikationsteilnehmers, insbesondere bei der Überprüfung der Authentizität eines Dienstanbieters, viele Daten zwischen den Kommunikationsteilnehmern übertragen werden müssen.

Somit liegt der Erfindung das Problem zugrunde, ein gegenüber dem bekannten Verfahren und der bekannten Anordnung vereinfachtes und verbessertes Verfahren sowie eine vereinfachte und verbesserte Anordnung zur Überprüfung einer Authentizität eines Kommunikationsteilnehmers in einem Kommunikationsnetz anzugeben.

Das Problem wird durch die Verfahren sowie durch die Anordnungen mit den Merkmalen gemäß den unabhängigen Patentansprüchen gelöst.

Bei dem Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz wird bei dem ersten Kommunikationsteilnehmers unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation gebildet. Bei einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz wird unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe

eine zweite Fehlerinformation gebildet. Unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation wird die Authentizität des ersten Kommunikationsteilnehmers überprüft.

5

Bei der Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz ist der erste Kommunikationsteilnehmer derart eingerichtet, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe eine erste Fehlerinformation bildbar ist. Ferner weist die Anordnung einen zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz auf, der derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist. Unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation ist die Authentizität des ersten Kommunikationsteilnehmers überprüfbar.

20

Unter der Überprüfung der Authentizität eines Kommunikationsteilnehmers in einem Kommunikationsnetz sind Verfahrensschritte zu verstehen, die im weiteren Sinn mit einer Überprüfung einer Berechtigung eines Kommunikationsteilnehmers zum Zugang zu einem Kommunikationsnetz oder einer Teilnahme an einer Kommunikation in einem Kommunikationsnetz durchgeführt werden.

25

Somit werden sowohl solche Verfahrensschritte umfaßt, die im Rahmen einer Überprüfung der Berechtigung eines Kommunikationsteilnehmers zum Zugang zu einem Kommunikationsnetz durchgeführt werden, als auch solche Verfahrensschritte umfaßt, die im Rahmen einer Bearbeitung oder einer Verwaltung von Daten, die bei der Überprüfung verwendet werden, durchgeführt werden.

30

35

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

5 Die im weiteren beschriebenen Weiterbildungen beziehen sich sowohl auf das Verfahren und die Anordnung.

Die Erfindung und die im weiteren beschriebenen Weiterbildungen können sowohl in Software als auch in Hardware, beispielsweise unter Verwendung einer speziellen elektrischen
10 Schaltung realisiert werden.

In einer Ausgestaltung ist der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstanutzer in dem Kommunikationsnetz.
15

Bevorzugt wird als Fehlererkennungsangabe eine Sequenzfolgenummer verwendet.

20 In einer Ausgestaltung ist die Information über die Zufallsangabe eine Zufallszahl.

In einer Weiterbildung wird die Prüfung der Authentizität dadurch vereinfacht, daß eine Differenz zwischen der Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und der
25 Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.

In einer Ausgestaltung wird die Prüfung der Authentizität dadurch hinsichtlich der Sicherheit des Kommunikationsnetzes
30 weiter verbessert, daß die Differenz beschränkt wird

Bevorzugt wird eine Weiterbildung im Rahmen eines Mobilfunksystems eingesetzt. Bei dem Mobilfunksystem sind/ist der Dienstanutzer als Mobiltelefon und/oder der Dienstanbieter als
35 Mobilfunknetzbetreiber realisiert.

In Figuren ist ein Ausführungsbeispiel der Erfindung dargestellt, welches im weiteren näher erläutert wird.

Es zeigen

5

Figur 1 ein Mobilfunksystem;

10

Figur 2 eine Skizze, in welcher symbolhaft eine Überprüfung einer Authentizität eines Kommunikationsteilnehmers dargestellt ist;

15

Figur 3 ein Ablaufdiagramm, in dem einzelne Verfahrensschritte bei einer Überprüfung einer Authentizität eines Dienstansbieters in einem Kommunikationsnetz dargestellt sind;

20

Figur 4 eine Skizze, in welcher symbolhaft eine Überprüfung einer Authentizität eines Kommunikationsteilnehmers gemäß dem 3G TS 33.102 Version 3.0.0-Standard dargestellt ist.

Ausführungsbeispiel: Mobilfunksystem

25

In Fig.1 ist ein Mobilfunksystem 100 dargestellt. Das Mobilfunksystem 100 umfaßt ein Mobiltelefon 101, ein lokales Einwählnetz 102 mit einem Einwählnetzbetreiber 103 und ein Heimatnetz 104 mit einem Heimatnetzbetreiber 105.

30

Bei dem Heimatnetz 104 ist das Mobiltelefon 101 angemeldet und registriert.

35

Ferner weisen das Mobiltelefon 101, das Einwählnetz 102 und das Heimatnetz 104 jeweils eine zentrale Verarbeitungseinheit 106, 107, 108 mit einem Speicher 109, 110, 111 auf, mit welchen Verarbeitungseinheiten 106, 107, 108 die im folgenden beschriebene Vorgehensweise überwacht und gesteuert wird und

auf welchen Speichern 109, 110, 111 Daten gespeichert werden und/oder sind.

Das Einwählnetz 102 und das Heimatnetz 104 sind über eine Datenleitung 112, über welche digitale Daten übertragen werden können, miteinander verbunden. Das Mobiltelefon 101 und das Einwählnetz 102 sind über ein beliebiges Übertragungsmedium 113 zur Übertragung von digitalen Daten miteinander verbunden.

10

In Fig.2 ist die Vorgehensweise bei einer Überprüfung einer Authentizität des Mobiltelefons 101 und die Vorgehensweise bei einer Überprüfung der Authentizität des Heimatnetzes 104 bzw. des Heimatnetzbetreibers 105 symbolhaft dargestellt und wird im folgenden kurz und auszugsweise erläutert.

15

Eine Übertragung von Daten ist in Fig.2 jeweils durch einen Pfeil dargestellt. Eine Richtung eines Pfeils kennzeichnet eine Übertragungsrichtung bei einer Datenübertragung.

20

Die im folgende beschriebene und in Fig.2 symbolhaft dargestellte Vorgehensweise basiert auf einem sogenannten 3G TS 33.102 Version 3.0.0-Standard, welcher eine Sicherheits-Architektur eines Mobilfunksystems beschreibt und in [1] beschrieben ist.

25

Bei einer Kommunikation wählt sich das Mobiltelefon 201 in das Einwählnetz 203 ein. Zu Beginn der Kommunikation erfolgt eine Überprüfung sowohl der Authentizität des Mobiltelefon 201 als auch der Authentizität des Heimatnetzes 204 bzw. des Heimatnetzbetreibers.

30

Dazu fordert das Einwählnetz 203 Authentifikationsdaten, mit welchen die Überprüfung der Authentizität des Nutzers 201 und des Heimatnetzes 204 bzw. des Heimatnetzbetreibers möglich ist, von dem Heimatnetz 204 an 211.

35

Die Authentifikationsdaten, welche von dem Heimatnetz 204 ermittelt werden, umfassen eine Zufallszahl und eine Sequenzfolgennummer des Heimatnetzes 204 (vgl. Fig.3 Schritt 310).

Die Sequenzfolgennummer des Heimatnetzes 204 wird derart ermittelt, daß ein Zähler des Heimatnetzes 204 bei jedem Kommunikationsversuch zwischen dem Mobiltelefon 201 und dem Heimatnetz 204 die Sequenzfolgennummer des Heimatnetzes 204 um den Wert 1 erhöht.

Es ist anzumerken, daß die Zufallszahl und die Sequenzfolgennummer des Heimatnetzes 204 nur einen Teil der Authentifikationsdaten darstellen und nicht abschließend zu verstehen sind. Weitere Authentifikationsdaten sind in [1] genannt.

Das Heimatnetz 204 überträgt die angeforderten Authentifikationsdaten an das Einwählnetz 203 212. Das Einwählnetz 203 bearbeitet die empfangenen Authentifikationsdaten in geeigneter Weise 213 und überträgt die bearbeiteten Authentifikationsdaten an das Mobiltelefon 201 214.

20

Das Mobiltelefon 201 überprüft unter Verwendung einer eigenen Sequenzfolgennummer, welche entsprechend der Sequenzfolgennummer des Heimatnetzes 204 gehandhabt wird, und der Sequenzfolgennummer des Heimatnetzes 204 die Authentizität des Heimatnetzes 204 215. Entsprechend des Heimatnetzes 204 weist das Mobiltelefon 201 ebenfalls einen Zähler auf.

Die Vorgehensweise bei der Überprüfung der Authentizität des Heimatnetzes 204 ist in [1] beschrieben. Davon abweichende Verfahrensschritte sind im folgenden beschrieben.

Im Rahmen der Überprüfung der Authentizität des Heimatnetzes 203 wird eine sogenannte Überlaufprüfung des Zählers des Mobiltelefons 201 durchgeführt. Durch diese Überlaufprüfung wird ein Überlauf eines zulässigen Zahlenbereichs des Zählers des Mobiltelefons 201 verhindert.

Bei der Überlaufprüfung werden folgende Bedingungen geprüft:

1) Sequenzfolgennummer des Heimatnetzes 204 > Sequenzfolgennummer des Mobiltelefons 201;

5

2) Sequenzfolgennummer des Heimatnetzes 204 - Sequenzfolgennummer des Mobiltelefons 201 < vorgebbare Abweichung (hier: 1000000);

10 wobei für die vorgebbare Abweichung gilt:

- vorgebbare Abweichung hinreichend groß, um im normalen bzw. störungsfreien Kommunikationsbetrieb auszuschließen, daß:

15

Sequenzfolgennummer des Heimatnetzes 204 - Sequenzfolgennummer des Mobiltelefons 201 > vorgebbare Abweichung;

- max. zulässige Sequenzfolgennummer des Mobiltelefon

20 201/vorgebbare Abweichung hinreichend groß, um auszuschließen, daß die max. zulässige Sequenzfolgennummer des Mobiltelefon 201 im Betrieb erreicht wird.

25 Ein Ergebnis der Überprüfung der Authentizität des Heimatnetzes 204, "Authentizität in Ordnung" 216, "Authentizität in Ordnung, aber ein Sequenzfehler aufgetreten" 217 oder "Authentizität nicht in Ordnung" 218, wird von dem Mobiltelefon 201 an das Heimatnetz 204 übertragen 419.

30 Bei dem Ergebnis "Authentizität in Ordnung" 216 überprüft das Einwählnetz 203, wie es in [1] beschrieben ist, die Authentizität des Mobiltelefons 201 220.

35 Bei dem Ergebnis "Authentizität nicht in Ordnung" 218 wird die Kommunikation unterbrochen oder neu begonnen 221.

Bei dem Ergebnis "Authentizität in Ordnung, aber ein Sequenzfehler aufgetreten" 217 erfolgt eine Resynchronisation 222. Unter Resynchronisation ist eine Änderung der Sequenzfolgennummer des Heimatnetzes 204 zu verstehen.

5

Dazu überträgt das Mobiltelefon 201 Resynchronisationsdaten an das Einwählnetz 203 222.

10

Die Resynchronisationsdaten umfassen dieselbe Zufallszahl, die im Rahmen der Authentifikationsdaten übertragen wurde, sowie die Sequenzfolgennummer des Mobiltelefons 201 (vgl. Fig.3 Schritt 320).

15

Das Einwählnetz 203 bearbeitet die Resynchronisationsdaten in geeigneter Weise und überträgt die bearbeiteten Resynchronisationsdaten an das Heimatnetz 204.

20

Das Heimatnetz überprüft unter Verwendung der bearbeiteten Resynchronisationsdaten die Sequenzfolgennummer des Mobiltelefons 201 und die Sequenzfolgennummer des Heimatnetzes 204 und verändert gegebenenfalls die Sequenzfolgennummer des Heimatnetzes 204 223 (vgl. Fig.3 Schritt 330).

25

Anschließend überträgt das Heimatnetz 204 neue Authentifikationsdaten, welche gegebenenfalls die veränderte Sequenzfolgennummer des Heimatnetzes 204 umfassen, an das Einwählnetz 203.

30

Zur Veranschaulichung der beschriebenen Vorgehensweise sind in Fig.3 wichtige Schritte 300 der Vorgehensweise dargestellt.

35

Fig.3 zeigt einen ersten Schritt 310, im Rahmen dessen die Authentifikationsdaten (erste Fehlerinformation) ermittelt werden.

Im Rahmen eines zweiten Schritts 320 werden die Resynchronisationsdaten (zweite Fehlerinformation) ermittelt.

5 Im Rahmen eines dritten Schritts 330 werden unter Verwendung der Resynchronisationsdaten die Sequenzfolgennummer des Mobiltelefons und die Sequenzfolgennummer des Heimatnetzes überprüft.

10 Im folgenden wird eine Alternative des ersten Ausführungsbeispiels beschrieben.

Bei dem alternativen Ausführungsbeispiel ist ein Verfahren realisiert, mit dem das Heimatnetz gegenüber einem Datenverlust bei einem Systemabsturz sicherer gemacht wird.

15

Dazu wird jeweils in einem vorgebbaren zeitlichen Abstand die aktuelle Sequenzfolgennummer des Heimatnetzes in dem Speicher des Heimatnetzes gespeichert. Eine bei einem Systemabsturz des Heimatnetzes verloren gegangene Sequenzfolgennummer des Heimatnetzes wird derart wiederhergestellt, daß zu dem Wert der gespeicherten Sequenzfolgennummer ein vorgebbarer Aufschlagswert addiert wird. Der vorgebbare Aufschlagswert ist derart bemessen, daß ein Überschreiten der Summe aus Sequenzfolgennummer des Mobiltelefons und vorgebbare Abweichung nicht
20
25 überschritten wird.

Bei dem alternativen Ausführungsbeispiel wird der vorgebbare Aufschlagswert derart bestimmt, daß eine durchschnittliche, aus Erfahrungswerten bei einem Betrieb des Kommunikationsnetzes bestimmte Zahl von Authentifikationsversuchen eines Tages
30 des Heimatnetzes mit einem Faktor mit dem Wert 10 multipliziert wird.

In diesem Dokument ist folgende Veröffentlichung zitiert:

- [1] 3G TS 33.102 Version 3.0.0-Draft-Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.

Patentansprüche

1. Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
 - 5 - bei dem bei dem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des Dienstanbieters und einer Information über eine Zufallsangabe eine erste Fehlerinformation gebildet wird;
 - bei dem bei einem zweiten Kommunikationsteilnehmer in dem
10 Kommunikationsnetz unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird;
 - bei dem unter Verwendung der ersten Fehlerinformation und
15 der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.
2. Verfahren nach Anspruch 1,
bei dem eine Differenz zwischen der Fehlererkennungsangabe
20 des ersten Kommunikationsteilnehmers und der Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.
3. Verfahren nach Anspruch 2,
25 bei dem die Differenz beschränkt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3,
eingesetzt im Rahmen eines Mobilfunksystems.
- 30 5. Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
 - bei der der erste Kommunikationsteilnehmer, derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer In-
35 formation über eine Zufallsangabe eine erste Fehlerinformation bildbar ist;

- bei der ein zweiter Kommunikationsteilnehmer in dem Kommunikationsnetz derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist;
 - bei der unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüfbar ist.
6. Anordnung nach Anspruch 5,
bei der der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstinutzer in dem Kommunikationsnetz sind/ist.
7. Anordnung nach Anspruch 5 oder 6,
bei der eine Fehlererkennungsangabe eine Sequenzfolgenummer ist.
8. Anordnung nach einem der Ansprüche 5 bis 7,
bei der die Information über die Zufallsangabe eine Zufallszahl ist.
9. Anordnung nach einem der Ansprüche 5 bis 8,
bei der der erste Kommunikationsteilnehmer ein Dienstanbieter in dem Kommunikationsnetz und/oder der zweite Kommunikationsteilnehmer ein Dienstinutzer in dem Kommunikationsnetz sind/ist.
10. Anordnung nach Anspruch 9,
bei der der Dienstanbieter ein Mobilfunkbetreiber und/oder der Dienstinutzer ein Mobiltelefon sind/ist.
11. Anordnung nach einem der Ansprüche 5 bis 10,
eingesetzt im Rahmen eines Mobilfunksystems.

Zusammenfassung**Verfahren und Anordnung zur Überprüfung einer Authentizität
eines ersten Kommunikationsteilnehmers in einem Kommunikati-
5 onsnetz**

Bei dem Verfahren und der Anordnung zur Überprüfung einer Au-
thentizität eines ersten Kommunikationsteilnehmers in einem
Kommunikationsnetz wird bei dem ersten Kommunikationsteilneh-
10 mer unter Verwendung einer Fehlererkennungsangabe des ersten
Kommunikationsteilnehmers und einer Information über eine Zu-
fallsangabe eine erste Fehlerinformation gebildet. Bei einem
zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz
wird unter Verwendung einer Fehlererkennungsangabe des zwei-
15 ten Kommunikationsteilnehmers und der Information über die
Zufallsangabe eine zweite Fehlerinformation gebildet. Unter
Verwendung der ersten Fehlerinformation und der zweiten Feh-
lerinformation wird die Authentizität des ersten Kommunikati-
onsteilnehmers überprüft.

20

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

REC'D 25 SEP 2001

WIPO

PCT

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 9P2055P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE00/01788	Internationales Anmeldedatum (Tag/Monat/Jahr) 31/05/2000	Prioritätsdatum (Tag/Monat/Tag) 15/06/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04Q7/38		
Anmelder SIEMENS AKTIENGESELLSCHAFT		



- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

 Diese Anlagen umfassen insgesamt drei Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 25/10/2000	Datum der Fertigstellung dieses Berichts 21.09.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Rabe, M Tel. Nr. +49 89 2399 8801 

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-13 ursprüngliche Fassung

Patentansprüche, Nr.:

1-11 eingegangen am 03/07/2001 mit Schreiben vom 02/07/2001

Zeichnungen, Blätter:

1/4-4/4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/01788

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-11
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-11
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-11
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Es wird auf die folgenden Dokumente verwiesen:

D1: US-A-5 799 084

D2: WO 91/01067

A. Bemerkungen zu Abschnitt V:

1. Die Erfindung bezieht sich auf ein **Verfahren** zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz, sowie auf eine entsprechende **Anordnung** gemäß den Merkmalen von **Anspruch 1 bzw. 5**.
2. Ein Verfahren und eine entsprechende Anordnung zur Überprüfung der Authentizität eines Kommunikationsteilnehmers, insbesondere eines Dienstanbieters oder eines Dienstinutzers, in einem Kommunikationsnetz sind z.B. aus dem Standard **3G TS 33.102 Version 3.0.0-Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999** bekannt.

Das Dokument **D1** beschreibt ein Verfahren zur Überprüfung der Authentizität eines Kommunikationsteilnehmers (Mobilstation) durch eine Basisstation. Die Mobilstation bildet dazu aus einer Zufallszahl und einer Folgenummer eine erste Authentifikationsnachricht, und sendet diese an die Basisstation. Die Basisstation berechnet ihrerseits unter Verwendung einer von ihr gebildeten Zufallszahl eine zweite Authentifikationsnachricht. Zur Überprüfung der Authentizität der Mobilstation werden die erste und zweite Authentifikationsnachricht in der Basisstation miteinander verglichen.

Darüber hinaus beschreibt das Dokument **D2** ein weiteres Verfahren zur Überprüfung der Authentizität eines Kommunikationsteilnehmers durch eine Basisstation, wobei von dem zu überprüfenden Kommunikationsteilnehmer eine Folgenummer und weitere Authentifikationsdaten (z.B. Seriennummer) gebildet und zur Basisstation übertragen werden. In der Basisstation werden ebenfalls eine Folgenummer und entsprechende Authentifikationsdaten gebildet, und mit den vom Kom-

munikationsteilnehmer übertragenen Daten verglichen.

3. Der vorliegenden Erfindung liegt die **Aufgabe** zugrunde, ausgehend von dem oben angegebenen Stand der Technik, ein vereinfachtes und verbessertes Verfahren sowie eine entsprechende Anordnung zur Überprüfung der Authentizität eines Kommunikationsteilnehmers anzugeben.
4. Zur **Lösung** dieser Aufgabe ist ein **Verfahren** zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz, sowie eine entsprechende **Anordnung** gemäß den Merkmalen von **Anspruch 1 bzw. 5** vorgesehen.

Die **Erfindung** besteht **im wesentlichen** darin, daß

- bei einem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, die von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation gebildet wird,
 - die erste Fehlerinformation von dem ersten Kommunikationsteilnehmer zu dem zweiten Kommunikationsteilnehmer übertragen wird,
 - bei dem zweiten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird, und
 - bei dem zweiten Kommunikationsteilnehmer unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.
5. Die Erfindung bietet den **Vorteil**, daß durch die Verwendung lediglich einer Information über die Zufallsangabe, die von dem zweiten Kommunikationsteilnehmer gebildet - und an den ersten Kommunikationsteilnehmer übertragen wird, ein geringerer Bedarf an Rechen- und Speicherleistung (zumindest) beim ersten Kommunikationsteilnehmer erforderlich ist, wodurch das Verfahren und die Anordnung zur Überprüfung der Authentizität vereinfacht werden.
 6. Der Gegenstand der **unabhängigen Ansprüche 1 und 5** wird daher als **neu** und

erfinderisch angesehen, Artikel 33 (2) und (3) PCT.

7. Die **Ansprüche 2 bis 4 und 6 bis 11** sind abhängig von Anspruch 1 bzw. 5 und erfüllen somit **ebenfalls** die Erfordernisse des Artikels 33 (2) und (3) PCT hinsichtlich **Neuheit** und **erfinderischer Tätigkeit**.
8. Die vorliegende Erfindung ist offensichtlich auch **gewerblich anwendbar**, Artikel 33 (4) PCT.

B. Bemerkungen zu Abschnitt VIII:

1. Damit die Erfordernisse der Regel 5.1 a) ii) PCT erfüllt werden, hätten in der Beschreibungseinleitung die Dokumente **D1** und **D2** angegeben werden sollen, die bezüglich der vorliegenden Anmeldung einen relevanten Stand der Technik darstellen; der darin enthaltene einschlägige Stand der Technik hätte kurz umrissen werden sollen.
2. Die Beschreibungseinleitung (inklusive der Aufgabenstellung und resultierenden Vorteile) hätte an die neu eingereichten Ansprüche angepaßt werden sollen, Regel 5.1 a) iii) PCT.
3. Um die Erfordernisse der Regel 6.3 b) PCT zu erfüllen, hätte jeder unabhängige Anspruch gegenüber dem nächstliegenden Stand der Technik (d.h. Dokument **D1**) deutlich in der **zweiteiligen Form** abgegrenzt werden sollen.
4. Um das Verständnis der Ansprüche zu erleichtern, hätten die in den Ansprüchen genannten technischen Merkmale mit in Klammern gesetzten Bezugszeichen versehen werden sollen, Regel 6.2 b) PCT. Dies gilt gleichermaßen für den Oberbegriff und den kennzeichnenden Teil.

C. Bemerkungen zu Abschnitt VIII:

1. Die Formulierungen "... bildbar ...", "... übertragbar ..." sowie "... überprüfbar ..." in

den Zeilen 9 und 16, bzw. 10 bis 11, bzw. 18 von Anspruch 5 sind aufgrund ihres fakultativen Charakters nicht klar, Artikel 6 PCT. Eine klarere Formulierung dieser Merkmale wäre erforderlich gewesen.

2. Die Beschreibung hätte in den Zeilen 22 bis 25 auf Seite 12 auf ihre Richtigkeit hin überprüft - und gegebenenfalls geändert werden sollen.

Patentansprüche

1. Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
 - 5 - bei dem bei dem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, welche von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation gebildet wird,
 - 10 - bei dem die erste Fehlerinformation von dem ersten Kommunikationsteilnehmer zu dem zweiten Kommunikationsteilnehmer übertragen wird,
 - 15 - bei dem bei dem zweiten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird;
 - 20 - bei dem bei dem zweiten Kommunikationsteilnehmer unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.
2. Verfahren nach Anspruch 1,
 - 25 bei dem eine Differenz zwischen der Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und der Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.
- 30 3. Verfahren nach Anspruch 2,
bei dem die Differenz beschränkt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3,
eingesetzt im Rahmen eines Mobilfunksystems.
- 35 5. Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,

- bei der der erste Kommunikationsteilnehmer derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, welche von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation bildbar ist und die erste Fehlerinformation zu dem zweiten Kommunikationsteilnehmer übertragbar ist;
- 10 - bei der der zweite Kommunikationsteilnehmer derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist und unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüfbar ist.

6. Anordnung nach Anspruch 5,
20 bei der der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

7. Anordnung nach Anspruch 5 oder 6,
25 bei der eine Fehlererkennungsangabe eine Sequenzfolgennummer ist.

8. Anordnung nach einem der Ansprüche 5 bis 7,
bei der die Information über die Zufallsangabe eine Zufallszahl ist.

9. Anordnung nach einem der Ansprüche 5 bis 8,
bei der der erste Kommunikationsteilnehmer ein Dienstanbieter in dem Kommunikationsnetz und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

16

10. Anordnung nach Anspruch 9,
bei der der Dienstanbieter ein Mobilfunkbetreiber und/oder
der Dienstinutzer ein Mobiltelefon sind/ist.

- 5 11. Anordnung nach einem der Ansprüche 5 bis 10,
eingesetzt im Rahmen eines Mobilfunksystems.

10

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 99P2055P	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE00/01788	International filing date (day/month/year) 31 May 2000 (31.05.00)	Priority date (day/month/year) 15 June 1999 (15.06.99)
International Patent Classification (IPC) or national classification and IPC H04Q 7/38		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1.	This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2.	This REPORT consists of a total of <u>7</u> sheets, including this cover sheet. <input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of <u>3</u> sheets.
3.	This report contains indications relating to the following items: <ul style="list-style-type: none"> I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input checked="" type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application

Date of submission of the demand 25 October 2000 (25.10.00)	Date of completion of this report 21 September 2001 (21.09.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE00/01788

I. Basis of the report

1. With regard to the **elements** of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages 1-13, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-11, filed with the letter of 03 July 2001 (03.07.2001)
- ☒ the drawings:
pages 1/4-4/4, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 00/01788

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1 - 11	YES
	Claims		NO
Inventive step (IS)	Claims	1 - 11	YES
	Claims		NO
Industrial applicability (IA)	Claims	1 - 11	YES
	Claims		NO

2. Citations and explanations

This report makes reference to the following documents:

D1: US-A-5 799 084

D2: WO-A-91/01067.

1. The invention pertains to a **method** for verifying the authenticity of a first communications participant in a communications network and to a corresponding **arrangement** according to the features of **Claims 1 and 5**, respectively.
2. A method and corresponding arrangement for verifying the authenticity of a communications participant, more particularly a service provider or a service user, in a communications network are known, for example, from the standard **3G TS 33.102 Version 3.0.0-Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999**.

Document **D1** describes a method for verifying the authenticity of a communications participant (mobile

.../...

(Continuation of V.2)

station) by means of a base station. To this end, the mobile station generates an authenticity message from a random number and a serial number and transmits it to the base station. The base station calculates a second authenticity message using a random number it has generated. The authenticity of the mobile station is verified by comparing the first and second authenticity messages in the base station.

In addition, document **D2** describes a further method for verifying the authenticity of a communications participant by means of a base station. In that method, the communications participant to be verified generates a serial number and further authenticity data (e.g., serial numbers) and transmits them to the base station. In the base station too, a serial number and further authenticity data are generated and compared with the data transmitted by the communications participant.

3. With the above-mentioned prior art as the point of departure, the **problem** to be solved by the present invention is to indicate a simplified, improved method and corresponding arrangement for verifying the authenticity of a communications participant.
4. The **solution** to this problem is a **method** for verifying the authenticity of a first communications participant in a communications network and a corresponding **arrangement** according to the features of **Claims 1 and 5**, respectively.

The **essential** aspects of the **invention** are that

.../...

(Continuation of V.2)

- a first communications participant generates a first error information using an error detection indication of the first communications participant and information concerning a random indication which was transmitted by a second communications participant in the communications network to the first communications participant,
 - the first error information is transmitted from the first communications participant to the second communications participant,
 - the second communications participant generates a second error information using an error detection indication of the second communications participant and the information concerning a random indication, and
 - the authenticity of the first communications participant is verified by the second communications participant using the first error information and the second error information.
5. The invention confers the **advantage** that, because of the use of only one information concerning the random indication, which is generated by the second communications participant and transmitted to the first communications participant, less calculating and storage capacity is required (at least) by the first communications participant; the method and arrangement for verifying authenticity are thereby simplified.

.../...

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 00/01788

(Continuation of V.2)

6. The subjects of **independent Claims 1 and 5** are therefore regarded as **novel** and **inventive** (PCT Article 33(2) and (3)).
7. **Claims 2 to 4 and 6 to 11** are dependent on Claims 1 and 5, respectively, and therefore **also** meet the requirements of PCT Article 33(2) and (3) with regard to **novelty** and **inventive step**.
8. The present invention is obviously also **industrially applicable** (PCT Article 33(4)).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Pursuant to PCT Rule 5.1(a)(ii), the introductory portion of the description should cite documents **D1** and **D2** and briefly outline the relevant prior art concerning the present application contained therein.
2. The introductory portion of the description (including the statement of problem and resulting advantages) should be brought into line with the newly filed claims (PCT Rule 5.1(a)(iii)).
3. Pursuant to PCT Rule 6.3(b), every independent claim should be clearly delimited in **two-part form** over the prior art (i.e., document **D1**).
4. To facilitate understanding of the claims, the technical features they contain should be followed by reference signs placed between parentheses (PCT Rule 6.2(b)). This applies equally to preamble and characterizing portion.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE 00/01788

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. The expressions "... can be generated ...", "... can be transmitted ..." and "... can be verified ..." in lines 9 and 16, 10 to 11, and 18 of Claim 5 are not clear because of their optional nature (PCT Article 6). These features should be defined more clearly.
2. The description, page 12, lines 22 to 25 should be checked for accuracy - and, if necessary, amended.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESEN

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

An:

SIEMENS AKTIENGESELLSCHAFT
Wittelsbacherplatz 2
80333 München
ALLEMAGNE

CT IPS AM Mch P/Ri

Eing. 27. Sep. 2001

GR
Frist

15.10.01

MITTEILUNG ÜBER DIE ÜBERSENDUNG
DES INTERNATIONALEN VORLÄUFIGEN
PRÜFUNGSBERICHTS

(Regel 71.1 PCT)

Absenderdatum
(Tag/Monat/Jahr)

21.09.2001

Aktenzeichen des Anmelders oder Anwalts

9P2055P

WICHTIGE MITTEILUNG

Internationales Aktenzeichen
PCT/DE00/01788

Internationales Anmeldedatum (Tag/Monat/Jahr)
31/05/2000

Prioritätsdatum (Tag/Monat/Jahr)
15/06/1999

Anmelder

SIEMENS AKTIENGESELLSCHAFT

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde

Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Finnie, A

Tel. +49 89 2399-8251



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT



(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 9P2055P	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE00/01788	Internationales Anmeldedatum (Tag/Monat/Jahr) 31/05/2000	Prioritätsdatum (Tag/Monat/Jahr) 15/06/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04Q7/38		
Anmelder SIEMENS AKTIENGESELLSCHAFT		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.
- ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).
- Diese Anlagen umfassen insgesamt drei Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 25/10/2000	Datum der Fertigstellung dieses Berichts 21.09.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Rabe, M Tel. Nr. +49 89 2399 8801 

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-13 ursprüngliche Fassung

Patentansprüche, Nr.:

1-11 eingegangen am 03/07/2001 mit Schreiben vom 02/07/2001

Zeichnungen, Blätter:

1/4-4/4 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE00/01788

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-11
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-11
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-11
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Es wird auf die folgenden Dokumente verwiesen:

D1: US-A-5 799 084

D2: WO 91/01067

A. Bemerkungen zu Abschnitt V:

1. Die Erfindung bezieht sich auf ein **Verfahren** zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz, sowie auf eine entsprechende **Anordnung** gemäß den Merkmalen von **Anspruch 1 bzw. 5**.
2. Ein Verfahren und eine entsprechende Anordnung zur Überprüfung der Authentizität eines Kommunikationsteilnehmers, insbesondere eines Dienstanbieters oder eines Dienstnutzers, in einem Kommunikationsnetz sind z.B. aus dem Standard **3G TS 33.102 Version 3.0.0-Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999** bekannt.

Das Dokument **D1** beschreibt ein Verfahren zur Überprüfung der Authentizität eines Kommunikationsteilnehmers (Mobilstation) durch eine Basisstation. Die Mobilstation bildet dazu aus einer Zufallszahl und einer Folgenummer eine erste Authentifikationsnachricht, und sendet diese an die Basisstation. Die Basisstation berechnet ihrerseits unter Verwendung einer von ihr gebildeten Zufallszahl eine zweite Authentifikationsnachricht. Zur Überprüfung der Authentizität der Mobilstation werden die erste und zweite Authentifikationsnachricht in der Basisstation miteinander verglichen.

Darüber hinaus beschreibt das Dokument **D2** ein weiteres Verfahren zur Überprüfung der Authentizität eines Kommunikationsteilnehmers durch eine Basisstation, wobei von dem zu überprüfenden Kommunikationsteilnehmer eine Folgenummer und weitere Authentifikationsdaten (z.B. Seriennummer) gebildet und zur Basisstation übertragen werden. In der Basisstation werden ebenfalls eine Folgenummer und entsprechende Authentifikationsdaten gebildet, und mit den vom Kom-

munikationsteilnehmer übertragenen Daten verglichen.

3. Der vorliegenden Erfindung liegt die **Aufgabe** zugrunde, ausgehend von dem oben angegebenen Stand der Technik, ein vereinfachtes und verbessertes Verfahren sowie eine entsprechende Anordnung zur Überprüfung der Authentizität eines Kommunikationsteilnehmers anzugeben.
4. Zur **Lösung** dieser Aufgabe ist ein **Verfahren** zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz, sowie eine entsprechende **Anordnung** gemäß den Merkmalen von **Anspruch 1 bzw. 5** vorgesehen.

Die **Erfindung** besteht im wesentlichen darin, daß

- bei einem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, die von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation gebildet wird,
 - die erste Fehlerinformation von dem ersten Kommunikationsteilnehmer zu dem zweiten Kommunikationsteilnehmer übertragen wird,
 - bei dem zweiten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird, und
 - bei dem zweiten Kommunikationsteilnehmer unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.
5. Die Erfindung bietet den **Vorteil**, daß durch die Verwendung lediglich einer Information über die Zufallsangabe, die von dem zweiten Kommunikationsteilnehmer gebildet - und an den ersten Kommunikationsteilnehmer übertragen wird, ein geringerer Bedarf an Rechen- und Speicherleistung (zumindest) beim ersten Kommunikationsteilnehmer erforderlich ist, wodurch das Verfahren und die Anordnung zur Überprüfung der Authentizität vereinfacht werden.
 6. Der Gegenstand der **unabhängigen Ansprüche 1 und 5** wird daher als **neu** und

erfinderisch angesehen, Artikel 33 (2) und (3) PCT.

7. Die **Ansprüche 2 bis 4 und 6 bis 11** sind abhängig von Anspruch 1 bzw. 5 und erfüllen somit **ebenfalls** die Erfordernisse des Artikels 33 (2) und (3) PCT hinsichtlich **Neuheit und erfinderischer Tätigkeit**.
8. Die vorliegende Erfindung ist offensichtlich auch **gewerblich anwendbar**, Artikel 33 (4) PCT.

B. Bemerkungen zu Abschnitt VIII:

1. Damit die Erfordernisse der Regel 5.1 a) ii) PCT erfüllt werden, hätten in der Beschreibungseinleitung die Dokumente **D1** und **D2** angegeben werden sollen, die bezüglich der vorliegenden Anmeldung einen relevanten Stand der Technik darstellen; der darin enthaltene einschlägige Stand der Technik hätte kurz umrissen werden sollen.
2. Die Beschreibungseinleitung (inklusive der Aufgabenstellung und resultierenden Vorteile) hätte an die neu eingereichten Ansprüche angepaßt werden sollen, Regel 5.1 a) iii) PCT.
3. Um die Erfordernisse der Regel 6.3 b) PCT zu erfüllen, hätte jeder unabhängige Anspruch gegenüber dem nächstliegenden Stand der Technik (d.h. Dokument **D1**) deutlich in der **zweiteiligen Form** abgegrenzt werden sollen.
4. Um das Verständnis der Ansprüche zu erleichtern, hätten die in den Ansprüchen genannten technischen Merkmale mit in Klammern gesetzten Bezugszeichen versehen werden sollen, Regel 6.2 b) PCT. Dies gilt gleichermaßen für den Oberbegriff und den kennzeichnenden Teil.

C. Bemerkungen zu Abschnitt VIII:

1. Die Formulierungen "... bildbar ...", "... übertragbar ..." sowie "... überprüfbar ..." in

den Zeilen 9 und 16, bzw. 10 bis 11, bzw. 18 von Anspruch 5 sind aufgrund ihres fakultativen Charakters nicht klar, Artikel 6 PCT. Eine klarere Formulierung dieser Merkmale wäre erforderlich gewesen.

2. Die Beschreibung hätte in den Zeilen 22 bis 25 auf Seite 12 auf ihre Richtigkeit hin überprüft - und gegebenenfalls geändert werden sollen.

Patentansprüche

1. Verfahren zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,
 - 5 - bei dem bei dem ersten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, welche von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation gebildet wird,
 - 10 - bei dem die erste Fehlerinformation von dem ersten Kommunikationsteilnehmer zu dem zweiten Kommunikationsteilnehmer übertragen wird,
 - 15 - bei dem bei dem zweiten Kommunikationsteilnehmer unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation gebildet wird;
 - bei dem bei dem zweiten Kommunikationsteilnehmer unter
20 Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüft wird.
2. Verfahren nach Anspruch 1,
 - 25 bei dem eine Differenz zwischen der Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und der Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers ermittelt wird.
- 30 3. Verfahren nach Anspruch 2,
bei dem die Differenz beschränkt wird.
4. Verfahren nach einem der Ansprüche 1 bis 3,
eingesetzt im Rahmen eines Mobilfunksystems.
- 35 5. Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz,

- bei der der erste Kommunikationsteilnehmer derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des ersten Kommunikationsteilnehmers und einer Information über eine Zufallsangabe, welche von einem zweiten Kommunikationsteilnehmer in dem Kommunikationsnetz zu dem ersten Kommunikationsteilnehmer übertragen wurde, eine erste Fehlerinformation bildbar ist und die erste Fehlerinformation zu dem zweiten Kommunikationsteilnehmer übertragbar ist;
- bei der der zweite Kommunikationsteilnehmer derart eingerichtet ist, daß unter Verwendung einer Fehlererkennungsangabe des zweiten Kommunikationsteilnehmers und der Information über die Zufallsangabe eine zweite Fehlerinformation bildbar ist und unter Verwendung der ersten Fehlerinformation und der zweiten Fehlerinformation die Authentizität des ersten Kommunikationsteilnehmers überprüfbar ist.

6. Anordnung nach Anspruch 5,

- bei der der erste Kommunikationsteilnehmer ein Dienstanbieter und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

7. Anordnung nach Anspruch 5 oder 6,

- bei der eine Fehlererkennungsangabe eine Sequenzfolgenummer ist.

8. Anordnung nach einem der Ansprüche 5 bis 7,

- bei der die Information über die Zufallsangabe eine Zufallszahl ist.

9. Anordnung nach einem der Ansprüche 5 bis 8,

- bei der der erste Kommunikationsteilnehmer ein Dienstanbieter in dem Kommunikationsnetz und/oder der zweite Kommunikationsteilnehmer ein Dienstnutzer in dem Kommunikationsnetz sind/ist.

10. Anordnung nach Anspruch 9,
bei der der Dienstanbieter ein Mobilfunkbetreiber und/oder
der Dienstinutzer ein Mobiltelefon sind/ist.

- 5 11. Anordnung nach einem der Ansprüche 5 bis 10,
eingesetzt im Rahmen eines Mobilfunksystems.